97

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/990,860	11/09/2001	James W. Kasper	062891.0668	2711

5073 7590 03/27/2006

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER	
ABYANEH, ALI S	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 03/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/990,860	KASPER ET AL.	
	Examiner	Art Unit	
	Ali S. Abyaneh	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37 and 39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-37 and 39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-39 are presented for examination.

2. Claim 38 is cancelled.

3. Claims 12, 13, 35 and 36 are amended.

Response to Arguments

4. Applicant's argument in regard to Perelson does not teach for each signature definition an inspector instance based on data file and does not generate executable code operable to detect intrusion is not persuasive. Perelson teaches creating protection files by generating and storing a plurality of test string/ inspector instance/executable code. In order to detect viral infection/intrusion the file to be screened is compared to each test string (see column 8, lines 12-53).

5. Applicant's amendments/arguments filed on 12-22-2005 have been fully considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) patent may not be obtained though the invention is not identically disclose or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-6, 8, 10, 11, 13-18, 28 and 31-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vimal Vaidya. (US Patent NO 6,279,113) in view of Alan S. Perelson et al. (US patent NO Re 36,417).

Regarding Claim 1

Vaidya teaches a method for intrusion detection of network traffic comprising: storing a data file comprising data defining one or more signature definition and one or more parameters and associated values (column8, lines 8-36); and executing signature definitions to detect network traffic matching the signature definition (column 6, lines 53-57). Vaidya does not explicitly teach **generating**, for each of the one or more signature definitions, an **inspector instance** based on the data file; and executing, for each of the one or more signature definitions, the **generated inspector instance** to detect network traffic matching the signature definition. However, in an analogous art Perleson teaches generating an inspector instance and executing the generated inspector instance to detect network traffic matching the signature definition (column 6, lines 6-24). Therefore it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Vaidya to include generating, for each of the one or more signature definitions, an inspector instance based on the data file; and executing, for each of the one or more signature definitions, the generated inspector instance to detect network traffic matching the signature definition. This would have been obvious because person

having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to prevent the spread of viruses and detect the newly introduced viruses and furthermore to match the plurality of contiguous digital signal of the test file to the plurality of contiguous digital signals of the original file (column 2, lines 8-12).

Regarding Claim 11

Vaidya teaches a method for use in intrusion detection comprising: storing a default signature file defining one or more default signatures (column 6, lines 53-56); storing a customized signature file defining one or more custom signatures (paragraph 3, lines 21-23); generating, for each of the one or more signatures defined in the default signature file, executable code operable to detect intrusions associated with the default signature (column 6, lines 11-14); executable code operable to detect intrusions associated with the custom signature (column 6, lines 11-14 and column 3, lines 21-23). Vaidya does not explicitly teach **Automatically generating, executable code operable to detect intrusions associated with the default signature** and generating, executable code operable to detect intrusions associated with the custom signature. However, in an analogous art, Perelson teaches a method wherein the executable codes are automatically generated (column 3, lines 5-24). Therefore it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Vaidya to include

Automatically generating, executable codes for default and customize signature. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to detect changes to the original computer file, where the original file has an associated protection file (column 2, lines 17-20).

Regarding Claim 28

Vaidya teaches a system for intrusion detection comprising: a sensor for detecting possible network intrusions, one or more engine groups each associated with one or more network detection engines (column 6, lines 57-67 and column 7, lines 1-11) a configuration handler comprising: a default signature file storing one or more signature definitions defining one or more respective default signatures for use by the sensor; and a user signature file storing a plurality of user-defined signatures for use by the sensor(column 6, lines 53-57); executable code based on either one of the stored default signatures or one of the stored user-defined signatures, the executable code operable to detect a network intrusion defined by the associated user-defined signature or the associated default signature (column 6, lines 11-13). Vaidya does not explicitly teach **generating an executable code.** However in an analogous art Perleson teaches generating an executable code to detect a network intrusion (column 6, lines 6-24). Therefor it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by

Vaidya to generate an executable code based on either one of the stored default signatures or one of the stored user-defined signatures, the executable code operable to detect a network intrusion defined by the associated user-defined signature or the associated default signature. This modification would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to prevent the spread of viruses and detect the newly introduced viruses and furthermore to match the plurality of contiguous digital signal of the test file to the plurality of contiguous digital signals of the original file (column 2, lines 8-12).

Regarding Claims 2, 3 and 4

Vaidya and Perleson teach all limitation of the claim as applied to claim 1 above. Vaidya furthermore teaches a method comprising: storing user data file comprising signature definitions, each modified signature definition comprising signature identifier associating the modified signature definition with a corresponding signature definition stored in the data file and for each signature definition, data comprising: a signature identification number parameter and associated value; a signature name and associated string; one or more parameters and respective values defining characteristics of the signature (column 9, lines 48-52) and each signature definition is stored in a separate line of data file (column 6, lines 53-57). Perleson furthermore teaches generating,

revised inspector instance based the modified signature definition and corresponding generated inspector instance (column 6, lines 6-24).

Regarding Claim 5

Vaidya and Perleson teach all limitation of the claim as applied to claim 2 above. Vaidya furthermore teaches a method, wherein the one or more modified signature definitions comprises modified values for associated modified parameters and no values indicative of the parameters in the corresponding signature definition that are not modified. (column 3, lines 1-11)).

Regarding Claim 6

Vaidya and Perleson teach all limitation of the claim as applied to claim 1 above. Vaidya furthermore teaches a method, wherein the data file comprises a file received from a sensor provider (column 6, lines 44-56).

Regarding Claim 8

Vaidya and Perleson teach all limitation of the claim as applied to claim 1 above. Vaidya furthermore teaches a method of receiving the data file at the sensor configuration handler (column 6, lines 37-40).

Regarding Claim 10

Vaidya and Perleson teach all limitation of the claim as applied to claim 1 above. Vaidya furthermore teaches a method comprising: storing a user data file comprising one or more user-defined signature definitions, each user-defined signature definition comprising a signature identifier not associated with any of the signature definitions in the data file (column 9, lines 48-52). Perleson furthermore teaches generating, for each of the user-defined signature definitions, an inspector instance based on the user defined signature (column 6, lines 6-24).

Regarding Claim 13

Vaidya and Perelson teach all limitation of the claim as applied to claim 11 above. Perleson furthermore teaches a method automatically generating, for each custom signature, executable code operable to detect intrusions associated with the custom signature based on the generated executable code of an associated default signature (column 6, lines 6-24).

Regarding Claim 14

Vaidya and Perelson teach all limitation of the claim as applied to claim 11 above. Zies furthermore teaches a method, wherein the one or more custom signatures comprises modifications of the default signatures (column 3, lines 61-67).

Regarding Claim 15

Vaidya and Perelson teach all limitation of the claim as applied to claim 11 above. Zies furthermore teaches a method, wherein generating, for each of the one or more default signatures, comprises generating executable code associated with the default signature based on an inspector shell (column 4, lines 51-56).

Regarding Claim 16

Vaidya and Perelson teach all limitation of the claim as applied to claim 15 above. Zies furthermore teaches a method, wherein the executable code associated with the default signature is operable to compare a plurality of parameter values to a plurality of parameter values defined by the default signature (paragraph 5, lines 16-23).

Regarding Claim 17

Vaidya and Perelson teach all limitation of the claim as applied to claim 11 above. Vaidya furthermore teaches a method, wherein the default signature file comprises, for each default signature; a signature identification number parameter and associated value; a signature name and associated string; and one or more parameters and respective values defining characteristics of the default signature (column 9, lines 48-52).

Regarding Claim 18

Vaidya and Perelson teach all limitation of the claim as applied to claim 11 above. Vaidya furthermore teaches a method, wherein the custom signature file comprises, for each signature; a signature identification number parameter and associated value; a signature name and associated string; and one or more parameters and respective values defining characteristics of the default signature (column 9, lines 48-52 and column 3, lines 21-23).

Regarding Claim 31

Vaidya and Perleson teach all limitation of the claim as applied to claim 28 above. Vaidya furthermore teaches a system, wherein handler further comprises a user interface operable to: receive an identification of a signature to be modified; the configuration provides a list of parameters and associated values for the signature to be modified (column 9, lines 48-52). Perleson furthermore teaches receiving revised values for one or more of the parameters; and write a revised signature to the user-defined data file (column 6, lines 6-24).

Regarding Claim 32 and 33

Vaidya and Perleson teach all limitation of the claim as applied to claim 28 above. Vaidya furthermore teaches a system, wherein the configuration handler further comprises a user interface operable to: provide a list of possible parameters for a particular engine; receive a plurality of values for one or more of

the parameters to define a user-defined signature associated with the engine; and parameters; write a user-defined signature to the user signature file and a reader and dispatcher to read data from default and user signature file and transmit to one or more engine (column 7, lines 11-30).

Regarding Claim 34

Vaidya and Perleson teach all limitation of the claim as applied to claim 28 above. Vaidya furthermore teaches a system further comprising a management console associated with the sensor and operable to communicate configuration data to the configuration handler and receive configuration help information from the configuration handler (column 7, lines 25-30).

8. Claims 7 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vimal Vaidya. (US Patent NO 6,279,113) in view of Alan S. Perelson et al. (US patent NO Re 36,417), further in view of Smaha et al. (US patent NO 5,557,742).

Regarding Claim 7 and 9

Vaidya and Perleson teach all limitation of the claim as applied to claim 1 and above. Vaidya and Perleson do not explicitly teach the data file comprises a file generated by a user and receiving configuration data file from a user and storing the received configuration data file in a user data file. However in an analogous art Smaha teaches the data file comprises a file generated by a user

and storing the received configuration data file in a user data file (paragraph 3, lines 54-64 and fig 4). Therefore it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Vaidya and Perleson to include generating the data file by a user and storing the received configuration data file in a user data file. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to enable the user to control the input mechanism and load a set of selected misuses (paragraph 9, lines 1-5)

9. Claims 12 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vimal Vaidya. (US Patent NO 6,279,113), in view of Alan S. Perelson (US Patent NO Re.36, 417), further in view of Kavin J. Ziese (US Patent NO 6,484,315).

Regarding Claim 12 and 29

Vaidya and Perleson teach all limitation of the claim as applied to claim 11 and 28 above. Vaidya and Perleson do not explicitly teach storing a customized signature file comprises storing modification of one or more of the default signature and configuration handler comprising stored modification to the default signatures. However, in an analogous art Ziese teaches storing a customized signature file comprises storing modification of one or more of the default signature and configuration handler comprising stored modification to the default

signatures (column 4, lines 51-67 and column 5, lines 1-2). Therefore it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Vaidya and Perleson to include storing modification of one or more of the default signature and configuration handler comprising stored modification to the default signatures. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to dynamically distribute intrusion detection update.

10. Claim 19-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Eva Chen et al. (US Patent NO.5, 960,170) in view of Kouznetsov (US Patent NO. 6,725,377).

Regarding Claim 19

Chen teaches a method for use in intrusion detection comprising: providing a sensor having a plurality of defined signatures (column 3, lines 57-59), and providing to the sensor a modified value for at least one of the parameters to create a modified signature (column 7, lines 34-40). Chen does not explicitly teach communicating to sensor a desire to create a modified signature and receiving from the sensor data indicative of parameters and associated values for the signature to be modified. However in an analogous art Kouznetsov teaches communicating to sensor a desire to create a modified signature and receiving from the sensor data indicative of parameters and

associated values for the signature to be modified (paragraph 7, lines 39-67). Therefore it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Chen to include communicating to sensor a desire to create a modified signature and receiving from the sensor data indicative of parameters and associated values for the signature to be modified. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to update recognize and detect new attacks and furthermore to update attack signature files either automatically or in accordance with user-set monitoring profiles (column 5, lines 19-21).

Regarding claim 20

Chen and Kouznetsov teach all limitation of the claim as applied to claim 19 above. Chen furthermore teaches a method comprising storing data associated with the modified signature in the sensor at a location separate from the associated unmodified signature (column 17, lines 24-25).

Regarding claim 21

Chen and Kouznetsov teach all limitation of the claim as applied to claim 20 above. Chen furthermore teaches storing in the sensor the name, signature identification number, and one or more parameters and associated values for the modified signature (column 13, lines1- 23 and fig 4c).

Regarding claim 22

Chen and Kouznetsov teach all limitation of the claim as applied to claim 19 above. Chen furthermore teaches communicating to the sensor the name of an engine associated with the signature (column 13, lines 1-23)

Regarding claim 23

Chen and Kouznetsov teach all limitation of the claim as applied to claim 20 above. Chen furthermore teaches storing plurality of parameter names and associated value (column 13, lines1- 23 and fig 4c).

Regarding claim 24

Chen and Kouznetsov teach all limitation of the claim as applied to claim 19 above. Chen furthermore teaches a method further comprising selecting a signature to be modified from the plurality of defined signatures (column 3, lines 28-35).

Regarding claim 25

Chen and Kouznetsov teach all limitation of the claim as applied to claim 22 above. Chen furthermore teaches a method comprising receiving a list indicative of all defined signatures associated with the engine (column 3, lines 57-60).

Regarding Claim 26 and 27

Chen and Kouznetsov teach all limitation of the claim as applied to claim 19 above. Chen furthermore teaches a method, wherein providing a sensor having a plurality of defined signatures comprises providing a sensor having a default data file defining the defined signatures and updating the default file (column 7, lines 62-67).

11. Claims 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vimal Vaidya. (US Patent NO 6,279,113), in view of Alan S. Perelson (US Patent NO Re.36, 417), in view of Kavin J. Ziese (US Patent NO 6,484,315), further in view of Smaha et al. (US patent NO 5,557,742).

Regarding Claim 30

Vaidya, Perleson and Ziese teach all limitation of the claim as applied to 29 above. Vaidya, Perleson and Ziese do not explicitly teach the stored modifications are stored in the user signature file. However, in an analogous art, Smaha teaches a system wherein the stored modifications are stored in the user signature file (paragraph 3, lines 54-64 and fig 4). Therefore it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Vaidya, Perleson and Ziese to store the modifications in the user signature file. This would have been obvious because

person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to enable the user to control the input mechanism and load a set of selected misuses (paragraph 9, lines 1-5).

12. Claim 35-37 and 39 are rejected under 35 U.S.C. 102(e) as being anticipated by Vimal Vaidya. (US Patent NO 6,279,113) in view of Bardsley (US Publication NO 2003/0061514).

Regarding Claim 35

Vaidya teaches a system for intrusion detection, comprising: a sensor for detecting possible network intrusions, the sensor comprising: at least one engine (column 7, lines 1-24); and a means for storing default signatures with parameter-value pairs associated with the default signatures (column 6, lines 53-57) and user-defined signatures with parameter-value pairs associated with the user-defined signatures for defining signature to be detected by the at least one engine (column 3, lines 21-22). Vaidya does not explicitly teach an engine parameter and an associated name for the engine parameter. However, in an analogous art, Bardsley teaches an engine parameter and an associated name for the engine parameter (paragraph [0024]-[0030]). Therefor it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Vaidya to include an engine parameter

and an associated name for the engine parameter. This modification would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to protect the network from any attacks and furthermore to decrease the likelihood that the intrusion detection server will fail or that troublesome queues and resulting delay will build (paragraph [0011]).

Regarding Claim 36

Vaidya teaches a method for use in intrusion detection of network traffic comprising: storing in a memory a signature definition associated with a signature to be detected (column 6, lines 53-56), the signature definitions comprising: an identifier for the signature; and one or more parameter-value pairs associated with the signature (column 9, lines 47-49), each parameter-value pair comprising a parameter name and associated parameter value (column 9, lines 49-60); and determining, based on the signature definition, the values that associated parameters of network traffic must take to meet the signature (column 10, lines 45-67 and column 11, lines 1-15). Vaidya does not explicitly teach an engine parameter and an associated name for the engine parameter. However, in an analogous art, Bardsley teaches an engine parameter and an associated name for the engine parameter (paragraph [0024]-[0030]). Therefor it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Vaidya to include an engine

parameter and an associated name for the engine parameter. This modification would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to protect the network from any attacks and furthermore to decrease the likelihood that the intrusion detection server will fail or that troublesome queues and resulting delay will build (paragraph [0011]).

Regarding Claim 37 and 39

Vaidya and Bardsley teach all limitation of the claim as applied to claim 36 above. Vaidya furthermore teaches a method, further comprising storing a plurality of signature definitions in a data file, each signature definition on a different line of the data file (column 6, lines 53-57) and each signature definition comprises an identification parameter preceding the signature (column 9 lines 47-61).

References Cited, Not Used

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

1. U.S. Patent No. 6,928,549

This reference relates to a method of operating an intrusion detection system that protects a computer system from intrusions by vandals such as hackers.

2. U.S. Patent No. 6,725,377

This reference relates to a computer program product and method that modifies anti-intrusion software on a computer network.

Conclusion

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali Abyaneh whose telephone number is (571) 272-7961. The examiner can normally be reached on Monday-Friday from (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 273-8300 Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ali Abyaneh A.A
Patent Examiner
Art Unit 2137
03/20/06

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER